瞭解AD同步的Umbrella加密

目錄

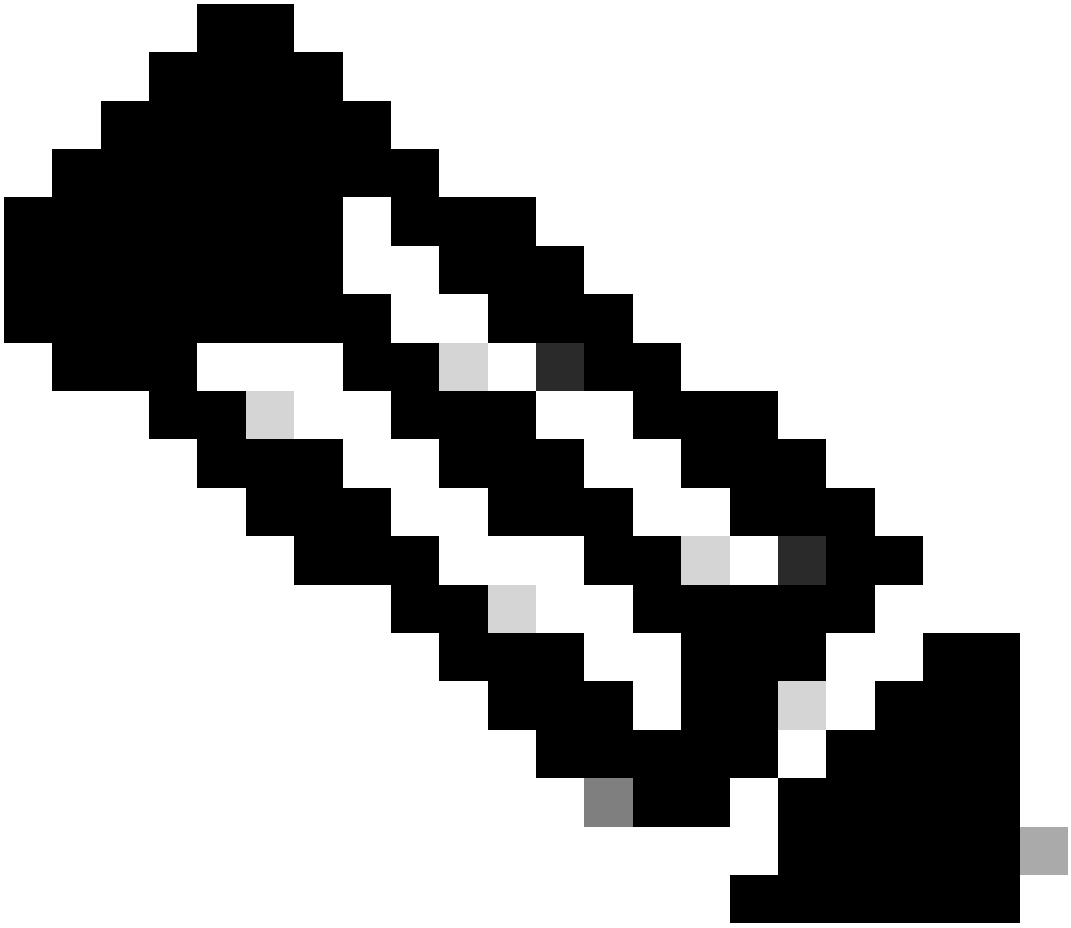
簡介

本檔案介紹適用於AD同步的Umbrella加密，例如此資料傳輸是如何加密的。

背景資訊

Umbrella AD Connector軟體使用LDAP從AD域控制器中檢索使用者、電腦和組資訊的詳細資訊。每個對象中僅儲存必要的屬性，其中包括sAMAccountName、dn、userPrincipalName、memberOf、objectGUID、primaryGroupId（用於使用者和電腦）以及primaryGroupToken（用於組）。

然後，此資料被上傳到Umbrella以便在策略配置和報告中使用。按使用者或按電腦過濾也需要此資料。



附註：objectGUID以雜湊形式傳送。

要確切瞭解正在同步的內容，您可以檢視以下內容中包含的.ldif檔案：

```
C:\Program Files\OpenDNS\OpenDNS Connector\ADSync\*.ldif
```

本文描述如何加密此資料傳輸。

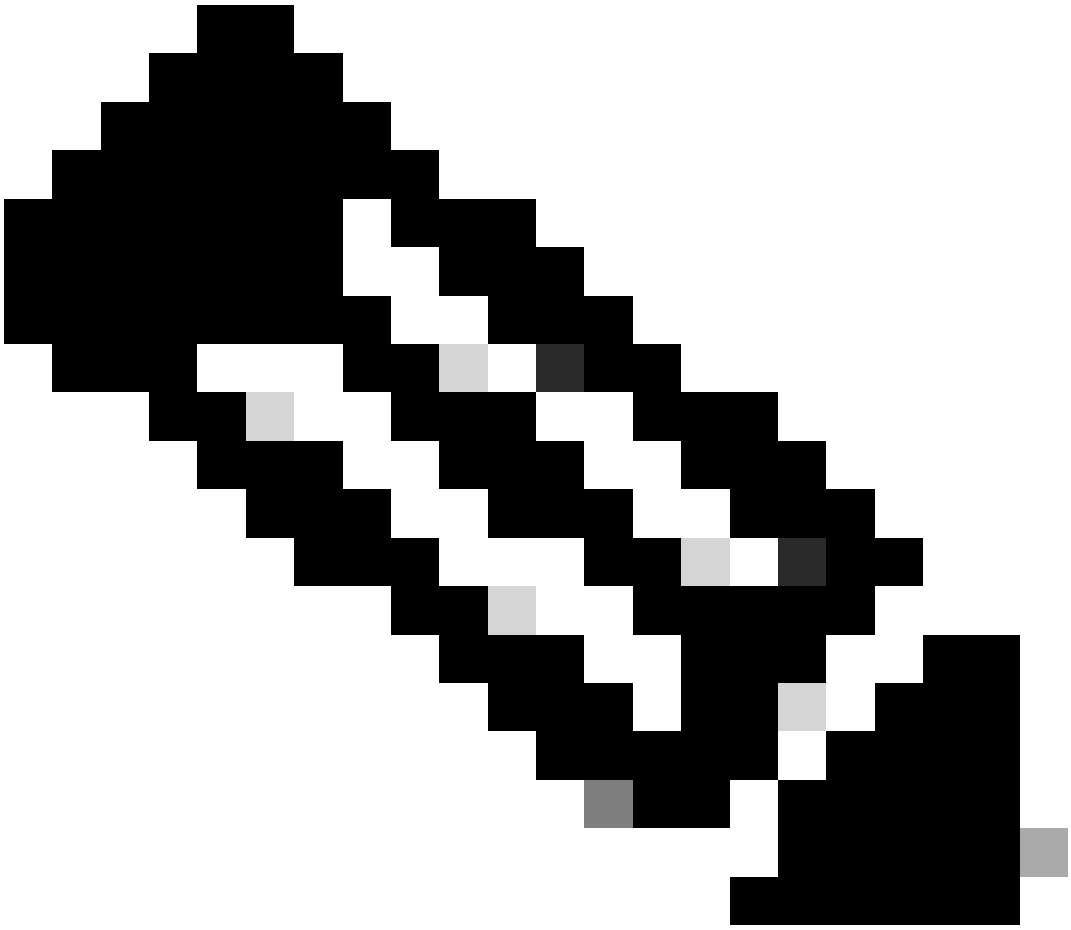
AD資料上傳加密

Umbrella AD聯結器使用安全的HTTPS連線將AD資訊上傳到Umbrella。Connector <> Umbrella雲之間的上傳始終是加密的。

AD資料檢索加密

從v1.1.22開始，聯結器現在嘗試在域控制器<>聯結器之間使用加密來檢索使用者詳細資訊。嘗試兩種方法：

- LDAPS。資料通過安全隧道傳輸。
- 採用Kerberos驗證的LDAP。提供資料包級別的加密。



附註：當聯結器軟體與用於ADsync的域控制器在同一伺服器上運行時，不使用LDAPS。

如果此嘗試由於任何原因而失敗，則會恢復為以下機制：

- 使用NTLM身份驗證的LDAP。這提供了安全身份驗證，但DC > Connector之間的資料傳輸是在不加密的情況下進行的。

為確保可以加密，我們建議：

- 在域控制器上啟用LDAPS。 這不屬於Umbrella支援的範圍，但可以使用Microsoft的文檔啟用。
- 確保在「Deployments > Sites and AD」中正確配置域控制器的主機名。這兩種加密方法都需要正確的主機名。如果主機名因任何原因不正確，我們建議使用我們的配置指令碼重新註冊域控制器，或者與Umbrella支援部門聯絡。

確認加密是否正在進行。您可以在此處檢查日誌檔案：

```
C:\Program Files (x86)\OpenDNS\OpenDNS Connector\<VERSION>\OpenDNSAuditClient.log
```

在AD同步期間，您會看到以下日誌條目：

LDAPS連線成功：
使用SSL進行<SERVER>通訊以獲取DN。

Kerberos驗證成功：
使用Kerberos進行<SERVER>通訊以獲取DN。

正在使用的NTLM故障回覆機制：
DC主機<SERVER>的Kerberos失敗。主機名可能無效。正在回退到NTLM查詢。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。